CLAIMS

What is claimed is:

1. A computer virus detection and containment system comprising:

at least one computer configured with at least one decoy address; and

a server operative to:

identify activity occurring at said computer, said activity involving said decoy address.

2. A system according to claim 1 wherein said server is operative to perform at least one virus containment action upon identifying said activity.

3. A system according to claim 2 wherein:

said server is operative to:

receive messages sent from said computer,

determine whether any of said messages are addressed to any of said decoy addresses, and

upon determining that at least one of said messages is addressed to any of said decoy addresses, perform said virus containment action.

4. A system according to claim 3 wherein said computer is configured to operate as said server.

5. A system according to claim 3 wherein said virus containment action is preventing any of said messages sent by said computer from being forwarded to their intended recipients.

6. A system according to claim 3 wherein said virus containment action is forwarding any of said messages that are addressed to a decoy address to a third party for analysis.

7. A system according to claim 3 wherein said virus containment action is notifying a user at said computer that at least one of said messages is addressed to any of said decoy addresses.

8. A system according to claim 3 wherein said virus containment action is notifying a system administrator that at least one of said messages is addressed to any of said decoy addresses.

9. A system according to claim 3 wherein said virus containment action is preventing any messages at said server from being forwarded to their intended destinations.

10. A system according to claim 3 wherein said virus containment action is revoking any privileges that said computer has to access a network.

11. A system according to claim 3 wherein said virus containment action is revoking any privileges that said computer has to access shared network files or directories.

12. A system according to claim 3 wherein said virus containment action is sending a command to a network device connected a network to block attempts by said computer to access said network.

13. A system according to claim 3 wherein said server is operative to buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

14. A system according to claim 13 wherein said virus containment action is changing said delay period for all of said messages sent by said computer and buffered by said server.

15. A system according to claim 13 wherein said virus containment action is changing said delay period for all messages buffered by said server.

16. A system according to claim 3 wherein said messages are electronic mail messages.

17. A computer virus detection and containment system comprising:

a computer configured with at least one decoy address and operative to periodically address a decoy message to one or more of said decoy addresses; and

a server operative to:

receive messages sent from said computer,

determine whether any of said messages are addressed to any of said decoy addresses, and

upon determining that at least one of said messages is addressed to any of said decoy addresses, determine whether said decoy-addressed message is a valid decoy message, and

upon determining that said decoy-addressed message is not a valid decoy message, perform at least one virus containment action.

18. A system according to claim 17 wherein said computer is configured to operate as said server.

19. A system according to claim 17 wherein said virus containment action is sending a command to a network device connected a network to block attempts by said computer to access said network.

20. A system according to claim 17 wherein said computer is operative to periodically send said decoy messages according to a schedule that is known in advance to said server.

21. A system according to claim 17 wherein at least one characteristic of said decoy message is known in advance to said server.

22. A system according to claim 17 wherein said computer is operative to send a plurality of decoy messages to a plurality of decoy addresses at various frequencies.

23. A system according to claim 17 wherein said server is operative to buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

24. A system according to claim 23 wherein said virus containment action is changing said delay period for all of said messages sent by said computer and buffered by said server.

25. A system according to claim 23 wherein said virus containment action is changing said delay period for all messages buffered by said server.

26. A system according to claim 17 wherein said messages are electronic mail messages.

27. A computer virus detection and containment system comprising:

a plurality of computers; and

a server operative to:

collect information regarding target behavior detected at any of said computers;

correlate said target behavior;

determine whether said correlated target behavior information corresponds to a predefined suspicious behavior pattern, and, if so;

perform at least one virus containment action.

28. A system according to claim 27 wherein any of said computers is configured with at least one target behavior profile, and wherein said configured computer is operative to detect said target behavior and report the presence of said target behavior to said server.

29. A system according to claim 27 wherein said server is configured with at least one target behavior profile, and wherein said server is operative to detect said target behavior at any of said computers.

30. A system according to claim 27 wherein any of said computers is configured to operate as said server.

31. A system according to claim 27 wherein said virus containment action is preventing any messages sent by any of said computers from being forwarded to their intended recipients.

32. A system according to claim 27 wherein said virus containment action is notifying a user at any of said computers that said suspicious behavior pattern has been detected.

33. A system according to claim 27 wherein said virus containment action is notifying a system administrator that said suspicious behavior pattern has been detected.

34. A system according to claim 27 wherein said virus containment action is revoking any privileges that any of said computers has to access a network.

35. A system according to claim 27 wherein said virus containment action is revoking any privileges that any of said computers has to access shared network files or directories.

36. A system according to claim 27 wherein said virus containment action is sending a command to a network device connected a network to block attempts by any of said computers to access said network.

37. A computer virus detection and containment system comprising:

a computer operative to send messages; and

a server operative to:

receive messages sent from said computer,

buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients; and

perform at least one virus containment action upon said buffer.

38. A system according to claim 37 wherein said virus containment action is preventing any of said messages sent by said computer from being forwarded from said buffer to their intended recipients.

39. A system according to claim 37 wherein said virus containment action is preventing any messages from being forwarded from said buffer to their intended destinations.

40. A system according to claim 37 wherein said virus containment action is changing said delay period for all of said messages sent by said computer and buffered by said server.

41. A system according to claim 37 wherein said virus containment action is changing said delay period for all messages buffered by said server.

42. A system according to claim 37 wherein said delay period is variably adjustable according to any of a plurality of desired levels of system alertness.

43. A system according to claim 37 wherein said delay period is variably adjustable according to any of a plurality of types of messages.

44. A system according to claim 37 wherein said delay period is variably adjustable according to any of a plurality of types of attachments.

45. A system according to claim 37 wherein said delay period is variably adjustable for different users.

46. A system according to claim 37 wherein said delay period is variably adjustable for different uses activities.

47. A system according to claim 37 wherein said delay period is variably adjustable for different destinations.

48. A system according to claim 37 wherein said server is operative to:

increase said delay period by a predetermined amount of time upon detecting suspected virus activity, and

perform said virus containment action if, during said increased delay period, additional suspected virus activity is detected and no indication that said activity is not virus related is received.

49. A system according to claim 48 wherein said server is operative to:

reduced said delay period to its previous level if, during said increased delay period, additional suspected virus activity is not detected.

50. A system according to claim 48 wherein said server is operative to:

reduced said delay period to its previous level if, during said increased delay period, an indication that said activity is not virus related is received.

51. A system according to claim 37 wherein said messages are electronic mail messages.

52. A computer virus detection and containment system comprising:

at least one computer configured with at least one decoy address; and

a server configured with said decoy address and operative to periodically send to said computer at least one decoy message addressed from said decoy address;

wherein said computer is operative to:

receive messages sent from said server,

determine whether any of said messages sent from said server are addressed from said decoy address, and

upon determining that at least one of said messages sent from said server is addressed from said decoy address, send a response decoy message addressed to said decoy address to said server in response to receiving said decoy message from said server, and

wherein said server is operative to:

receive messages sent from said computer,

determine whether any of said messages sent from said computer are addressed to said decoy address, and

upon determining that at least one of said messages sent from said computer is addressed to said decoy address, determine whether said decoy-addressed message is a valid decoy message, and

upon determining that said decoy-addressed message is not a valid decoy message, perform at least one virus containment action.

53. A system according to claim 52 wherein said response decoy message is the same as said decoy message received from said server.

54. A system according to claim 53 wherein said computer is operative to open said decoy message received from said server prior to sending said response decoy message to said server.

55. A system according to claim 53 wherein said computer is operative to open an attachment attached to said decoy message received from said server prior to sending said response decoy message to said server.

56. A system according to claim 52 wherein said computer is configured to operate as said server.

57. A system according to claim 52 wherein said virus containment action is preventing any messages at said server from being forwarded to their intended destinations.

58. A system according to claim 52 wherein said virus containment action is revoking any privileges that said computer has to access a network.

59. A system according to claim 52 wherein said virus containment action is revoking any privileges that said computer has to access shared network files or directories.

60. A system according to claim 52 wherein said virus containment action is sending a command to a network device connected a network to block attempts by said computer to access said network.

61. A system according to claim 52 wherein said server is operative to periodically send said decoy messages according to a schedule that is known in advance to said computer.

62. A system according to claim 52 wherein at least one characteristic of said decoy message sent to said computer is known in advance to said computer.

63. A system according to claim 52 wherein said server is operative to buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

64. A system according to claim 63 wherein said virus containment action is changing said delay period for all of said messages sent by said computer and buffered by said server.

65. A system according to claim 63 wherein said virus containment action is changing said delay period for all messages buffered by said server.

66. A system according to claim 52 wherein said messages are electronic mail messages.

67. A computer virus detection and containment system comprising:

a plurality of servers, each configured to maintain a virus detection sensitivity level; and

multiple pluralities of computers, each plurality of computers being in communication with at least one of said servers;

wherein each of said servers is operative to:

detect suspected virus activity at any of its related plurality of computers,

notify any of said servers of said detected suspected virus activity, and

adjust said virus detection sensitivity level according to a predefined plan.

68. A system according to claim 67 wherein said predefined plan is in predefined relation to said notification.

69. A system according to claim 67 wherein said adjustment is a lengthening of a message buffer delay period.

70. A system according to claim 67 wherein said adjustment is selecting virus containment actions which are performed when a suspected virus is detected at any of said computers.

71. A system according to claim 67 wherein said adjustment is selecting target behavior to be tracked at said computers.

72. A system according to claim 67 wherein said adjustment is selecting which correlations of target behavior are performed for target behavior detected at any of said computers.

73. A system according to claim 72 wherein said adjustment is selecting quantifications of suspicious behavior patterns.

74. A method for computer virus detection and containment, the method comprising:

configuring at least one computer with at least one decoy address; and

identifying activity occurring at said computer, said activity involving said decoy address.

75. A method according to claim 74 and further comprising performing at least one virus containment action upon identifying said activity.

76. A method according to claim 75 wherein:

said identifying step comprises:

receiving messages sent from said computer;

determining whether any of said messages are addressed to any of said decoy addresses; and

and wherein said performing step comprises performing upon determining that at least one of said messages is addressed to any of said decoy addresses.

77. A method according to claim 76 wherein said performing step comprises preventing any of said messages sent by said computer from being forwarded to their intended recipients.

78. A method according to claim 76 wherein said performing step comprises forwarding any of said messages that are addressed to a decoy address to a third party for analysis.

79. A method according to claim 76 wherein said performing step comprises notifying a user at said computer that at least one of said messages is addressed to any of said decoy addresses.

80. A method according to claim 76 wherein said performing step comprises notifying a method administrator that at least one of said messages is addressed to any of said decoy addresses.

81. A method according to claim 76 wherein said performing step comprises preventing any messages received from said computer from being forwarded to their intended destinations.

82. A method according to claim 76 wherein said performing step comprises revoking any privileges that said computer has to access a network.

83. A method according to claim 76 wherein said performing step comprises revoking any privileges that said computer has to access shared network files or directories.

84. A method according to claim 76 wherein said performing step comprises sending a command to a network device connected a network to block attempts by said computer to access said network.

85. A method according to claim 76 and further comprising buffering any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

86. A method according to claim 85 wherein said performing step comprises changing said delay period for all of said buffered messages sent by said computer.

87. A method according to claim 85 wherein said performing step comprises changing said delay period for all messages buffered by a server.

88. A method for computer virus detection and containment, the method comprising:

configuring a computer with at least one decoy address;

periodically sending a decoy message addressed to one or more of said decoy addresses;

receive messages sent from said computer;

determining whether any of said messages are addressed to any of said decoy addresses;

upon determining that at least one of said messages is addressed to any of said decoy addresses, determining whether said decoy-addressed message is a valid decoy message; and

upon determining that said decoy-addressed message is not a valid decoy message, performing at least one virus containment action.

89. A method according to claim 88 wherein said performing step comprises sending a command to a network device connected a network to block attempts by said computer to access said network.

90. A method according to claim 88 and further comprising configuring a server at which said messages are received with a schedule, and wherein said periodically sending step comprises sending said decoy messages according to said schedule.

91. A method according to claim 88 and further comprising configuring a server at which said messages are received with at least one characteristic of said decoy message.

92. A method according to claim 88 wherein said sending step comprises sending a plurality of decoy messages to a plurality of decoy addresses at various frequencies.

93. A method according to claim 88 and further comprising buffering any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

94. A method according to claim 93 wherein said performing step comprises changing said delay period for all of said messages sent by said computer and buffered by a server.

95. A method according to claim 93 wherein said performing step comprises changing said delay period for all messages buffered by a server.

96. A method for computer virus detection and containment, the method comprising:

collecting information regarding target behavior detected at any of a plurality of computers;

correlating said target behavior;

determining whether said correlated target behavior information corresponds to a predefined suspicious behavior pattern, and, if so;

performing at least one virus containment action.

97. A method according to claim 96 and further comprising:

configuring any of said computers with at least one target behavior profile; and

reporting the presence of said target behavior to a server.

98. A method according to claim 96 and further comprising:
configuring a server with at least one target behavior profile; and
detecting at said server said target behavior at any of said computers.

99. A method according to claim 96 wherein said performing step comprises preventing any messages sent by any of said computers from being forwarded to their intended recipients.

100. A method according to claim 96 wherein said performing step comprises notifying a user at any of said computers that said suspicious behavior pattern has been detected.

101. A method according to claim 96 wherein said performing step comprises notifying a method administrator that said suspicious behavior pattern has been detected.

102. A method according to claim 96 wherein said performing step comprises revoking any privileges that any of said computers has to access a network.

103. A method according to claim 96 wherein said performing step comprises revoking any privileges that any of said computers has to access shared network files or directories.

104. A method according to claim 96 wherein said performing step comprises sending a command to a network device connected a network to block attempts by any of said computers to access said network.

105. A method for computer virus detection and containment, the method comprising:
receiving messages sent from a computer,
buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients; and
perform at least one virus containment action upon said buffer.

106. A method according to claim 105 wherein said performing step comprises preventing any of said messages sent by said computer from being forwarded from said buffer to their intended recipients.

107. A method according to claim 105 wherein said performing step comprises preventing any messages from being forwarded from said buffer to their intended destinations.

108. A method according to claim 105 wherein said performing step comprises changing said delay period for all of said messages sent by said computer and buffered by a server.

109. A method according to claim 105 wherein said performing step comprises changing said delay period for all messages buffered by a server.

110. A method according to claim 105 wherein said performing step comprises variably adjusting said delay period according to any of a plurality of desired levels of method alertness.

111. A method according to claim 105 wherein said performing step comprises variably adjusting said delay period according to any of a plurality of types of messages.

112. A method according to claim 105 wherein said performing step comprises variably adjusting said delay period according to any of a plurality of types of attachments.

113. A method according to claim 105 wherein said performing step comprises variably adjusting said delay period for different users.

114. A method according to claim 105 wherein said performing step comprises variably adjusting said delay period for different uses activities.

115. A method according to claim 105 wherein said performing step comprises variably adjusting said delay period for different destinations.

116. A method according to claim 105 and further comprising:

increasing said delay period by a predetermined amount of time upon detecting suspected virus activity, and

wherein said performing step comprises performing if, during said increased delay period, additional suspected virus activity is detected and no indication that said activity is not virus related is received.

117. A method according to claim 116 and further comprising reducing said delay period to its previous level if, during said increased delay period, additional suspected virus activity is not detected.

118. A method according to claim 116 and further comprising reducing said delay period to its previous level if, during said increased delay period, an indication that said activity is not virus related is received.

119. A method for computer virus detection and containment, the method comprising:

configuring at least one computer and at least one server with at least one decoy address;

periodically sending from said server to said computer at least one decoy message addressed from said decoy address;

at said computer:

receiving messages sent from said server;

determining whether any of said messages sent from said server are addressed from said decoy address;

upon determining that at least one of said messages sent from said server is addressed from said decoy address, sending a response decoy message addressed to said decoy address to said server in response to receiving said decoy message from said server;

at said server:

receiving messages sent from said computer,

determining whether any of said messages sent from said computer are addressed to said decoy address;

upon determining that at least one of said messages sent from said computer is addressed to said decoy address, determining whether said decoy-addressed message is a valid decoy message; and

upon determining that said decoy-addressed message is not a valid decoy message, performing at least one virus containment action.

120. A method according to claim 119 wherein said sending a response step comprises sending said decoy message received from said server.

121. A method according to claim 120 wherein said sending a response step comprises opening said decoy message received from said server prior to sending said response decoy message to said server.

122. A method according to claim 120 wherein said sending a response step comprises opening an attachment attached to said decoy message received from said server prior to sending said response decoy message to said server.

123. A method according to claim 119 wherein said performing step comprises preventing any messages at said server from being forwarded to their intended destinations.

124. A method according to claim 119 wherein said performing step comprises revoking any privileges that said computer has to access a network.

125. A method according to claim 119 wherein said performing step comprises revoking any privileges that said computer has to access shared network files or directories.

126. A method according to claim 119 wherein said performing step comprises sending a command to a network device connected a network to block attempts by said computer to access said network.

127. A method according to claim 119 wherein said periodically sending step comprises periodically sending said decoy messages according to a schedule that is known in advance to said computer.

128. A method according to claim 119 wherein said configuring step comprises configuring said computer with at least one characteristic of said decoy message.

129. A method according to claim 119 and further comprising buffering at said server any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

130. A method according to claim 129 wherein said performing step comprises changing said delay period for all of said messages sent by said computer and buffered by said server.

131. A method according to claim 129 wherein said performing step comprises changing said delay period for all messages buffered by said server.

132. A computer virus detection and containment method comprising:

configuring each a plurality of servers to maintain a virus detection sensitivity level; and

providing multiple pluralities of computers, each plurality of computers being in communication with at least one of said servers;

detecting suspected virus activity at any of said plurality of computers,

notifying any of said servers of said detected suspected virus activity, and

adjusting said virus detection sensitivity level at any of said servers according to a predefined plan.

133. A method according to claim 132 wherein said adjusting step comprises adjusting where said predefined plan is in predefined relation to said notification.

134. A method according to claim 132 wherein said adjusting step comprises lengthening of a message buffer delay period.

135. A method according to claim 132 wherein said adjusting step comprises selecting virus containment actions which are performed when a suspected virus is detected at any of said computers.

136. A method according to claim 132 wherein said adjusting step comprises selecting target behavior to be tracked at said computers.

137. A method according to claim 132 wherein said adjusting step comprises selecting which correlations of target behavior are performed for target behavior detected at any of said computers.

138. A method according to claim 137 wherein said adjusting step comprises selecting quantifications of suspicious behavior patterns.